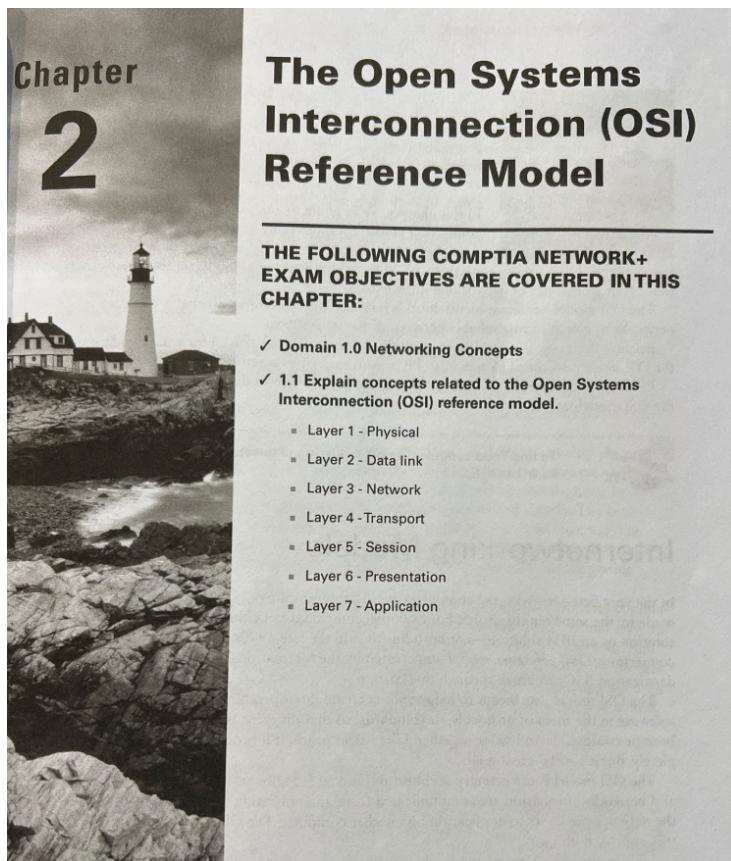


# Chapter 2 - The Open Systems Interconnection (OSI) Reference Model

#StudyGuideN10-009

#network



## 1 Objetivos del capítulo

- **Dominio:** 1.0 Networking Concepts
- **Objetivo del examen 1.1:** Explicar los conceptos relacionados con el **modelo de referencia OSI (Open Systems Interconnection)**.
- **Capas del modelo:**
  1. Physical
  2. Data Link
  3. Network
  4. Transport
  5. Session
  6. Presentation
  7. Application

## 2 Concepto general del modelo OSI

El modelo OSI es una **arquitectura jerárquica de siete capas** desarrollada por la **ISO (International Organization for Standardization)** a finales de los años 70.

Su objetivo fue **permitir la interoperabilidad entre sistemas de distintos fabricantes**, definiendo estándares comunes para el intercambio de datos.

 En esencia, el modelo OSI es una guía conceptual que describe cómo se comunican los sistemas a través de redes.

Cada capa del modelo tiene **funciones específicas**, y juntas proporcionan una estructura modular para el diseño y diagnóstico de redes.

## 3 Internetworking Models

En los primeros años de las redes, los ordenadores solo podían comunicarse con equipos del **mismo fabricante** (por ejemplo, DECnet o IBM Net).

El **modelo OSI** rompió esta limitación, promoviendo una comunicación abierta entre sistemas heterogéneos.

**Finalidad del modelo OSI:**

- Establecer un marco común de **protocolos y estándares**.
- Asegurar que distintos equipos y software **puedan interoperar**.
- Dividir la comunicación en capas con funciones bien definidas.

 El OSI es el modelo arquitectónico base que describe cómo los datos se transmiten desde una aplicación en un equipo hasta otra aplicación en un equipo remoto.

## 4 The Layered Approach

Un **reference model** actúa como **plano conceptual** que organiza las tareas de comunicación en **capas (layers)**.

Cada capa depende de la inferior y sirve a la superior, creando una arquitectura ordenada y modular.

**Ejemplo ilustrativo:**

Al crear una empresa, los departamentos (atención al cliente, inventario, envíos) trabajan de forma independiente pero coordinada. Cada uno tiene tareas y protocolos específicos.

De la misma manera, en el modelo OSI, cada capa tiene funciones definidas que permiten la comunicación eficiente entre sistemas.

**Ventaja clave:**

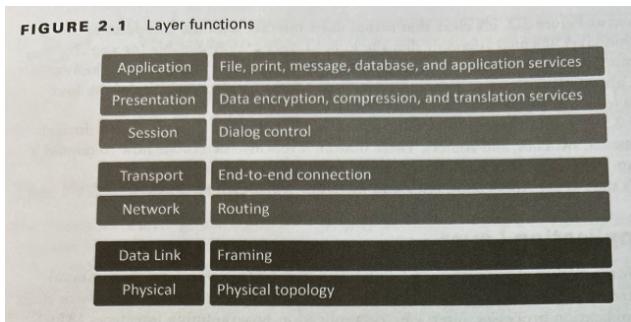
Si una capa cambia o se mejora, las demás no se ven afectadas, siempre que se mantengan las interfaces estándar entre ellas.

## 5 Ventajas de los Modelos de Referencia

1. **Estandarización de procesos:** define cómo debe ocurrir cada tipo de comunicación.
2. **Compatibilidad entre fabricantes:** equipos de distintos orígenes pueden operar juntos.
3. **Facilidad de diseño y mantenimiento:** se pueden desarrollar, probar o reemplazar capas de forma independiente.
4. **Diagnóstico estructurado:** permite aislar problemas de red identificando en qué capa ocurre el fallo.

## 6 Capas del modelo OSI

El modelo OSI no es físico, sino conceptual. Proporciona una **guía estructurada** para implementar tecnologías y protocolos.



Capa	Nombre	Función principal
7	Application	Servicios al usuario final (navegadores, correo, etc.)
6	Presentation	Traducción, compresión y cifrado de datos
5	Session	Control de diálogo entre aplicaciones
4	Transport	Conexión extremo a extremo y control de errores
3	Network	Direccionamiento lógico y enrutamiento
2	Data Link	Enlace físico y control de acceso al medio
1	Physical	Transmisión de bits por el medio físico

💡 Mnemónico útil: “**Please Do Not Throw Sausage Pizza Away**” (de la capa 1 a la 7).

💡 De la capa 1 → 7 (ascendente)

Mnemónico	Traducción aproximada
<b>Please Do Not Throw Sausage Pizza Away</b>	“Por favor, no tires la pizza de salchicha.”
<b>Please Do Not Teach Stupid People Anything</b>	“Por favor, no enseñas nada a la gente tonta.”
<b>People Don't Need Those Stupid Packets Anyway</b>	“La gente no necesita esos paquetes estúpidos de todos modos.”
<b>Please Don't Nap The Students' Projects Away</b>	“Por favor, no te duermas con los proyectos de los alumnos.”

💡 De la capa 7 → 1 (descendente)

Mnemónico	Traducción aproximada
<b>All People Seem To Need Data Processing</b>	“Todas las personas parecen necesitar procesar datos.”
<b>All Pros Search Top Notch Data Providers</b>	“Todos los profesionales buscan los mejores proveedores de datos.”
<b>All Penguins Should Take Nice Data Photos</b>	“Todos los pingüinos deberían tomar buenas fotos de datos.”

💡 En los exámenes de certificación (como Network+), el más usado es el clásico ascendente: “**Please Do Not Throw Sausage Pizza Away**” → Physical, Data Link, Network, Transport, Session, Presentation, Application.

## 7 Principio de agrupación

Las capas pueden agruparse en dos conjuntos:

**FIGURE 2.2** The upper layers

Application	Provides a user interface
Presentation	Presents data Handles processing such as encryption
Session	Keeps different applications' data separate

**FIGURE 2.3** The lower layers

Transport	Provides reliable or unreliable delivery Performs error correction before retransmit
Network	Provides logical addressing, which router user for path determination
Data Link	Combines packets into bytes and bytes into frames Provides access to media using MAC address Performed error detection, not correction
Physical	Move bits between devices Specifies voltage, wire speed, and pin-out of cables

Grupo	Capas	Descripción
Upper Layers	7–5	Cómo las aplicaciones se comunican entre sí y con los usuarios.
Lower Layers	4–1	Cómo los datos se transmiten físicamente a través de la red.

## 8 Application Layer (Capa 7)

La **Application Layer** es la capa superior del modelo OSI.

Es el punto de contacto más cercano entre los **usuarios finales y la red**, proporcionando los **servicios y protocolos** que permiten a las aplicaciones comunicarse a través de ella.

Esta capa **no incluye las aplicaciones en sí**, sino los **protocolos que usan** para acceder a los recursos de red.

 La capa de aplicación define qué operaciones pueden realizar las aplicaciones, cómo inician la comunicación y qué formato de datos intercambian.

### ◆ Funciones principales

#### 1. Interfaz entre el software y la red:

Permite a las aplicaciones acceder a los servicios de red, como la transferencia de archivos, el correo electrónico o la navegación web.

#### 2. Detección de recursos y disponibilidad:

Verifica que el servidor o dispositivo remoto esté disponible antes de iniciar la sesión (por ejemplo, mediante DNS o un handshake de aplicación).

#### 3. Coordinación de procesos y recuperación:

Si una comunicación falla, el protocolo de aplicación puede reiniciar o continuar la transferencia sin intervención del usuario (como FTP o HTTP).

#### 4. Gestión de errores a nivel de aplicación:

Aunque las capas inferiores manejan la entrega, la capa 7 puede generar mensajes de error específicos del servicio (por ejemplo, códigos 404 o 500 en HTTP).

### ◆ Protocolos y servicios comunes

Protocolo	Descripción
HTTP / HTTPS	Transferencia de páginas web y contenido multimedia. HTTPS agrega cifrado TLS.
FTP / TFTP	Transferencia de archivos; TFTP es una versión simplificada sin autenticación.
SMTP / POP3 / IMAP	Envío y recepción de correo electrónico.
DNS	Traducción de nombres de dominio a direcciones IP.
Telnet / SSH	Acceso remoto a dispositivos (SSH agrega cifrado).
SNMP	Supervisión y gestión de dispositivos de red.

 Los navegadores, clientes de correo y gestores de red “usan” estos protocolos, pero no forman parte de la capa 7.

## ◆ Ejemplo práctico

Cuando un usuario descarga un archivo por **FTP**:

1. El cliente FTP inicia sesión con el servidor (usuario/contraseña).
2. La capa de aplicación coordina la solicitud del archivo.
3. Los datos se transfieren en modo binario o texto según el formato definido.
4. Si se interrumpe, puede reanudar la transferencia gracias al control propio del protocolo.

El resto de capas (6 → 1) se encarga del transporte físico de los datos.

## 9 Presentation Layer (Capa 6)

La **Presentation Layer** se centra en el **formato y la representación de los datos**.

Actúa como un **traductor universal** que convierte la información de la aplicación en un formato estándar para la red y viceversa.

Su propósito es garantizar que el emisor y el receptor **interpreten los datos del mismo modo**, sin importar diferencias de hardware o sistema operativo.

 La capa 6 asegura que “los datos tengan sentido” cuando llegan al destino.

## ◆ Funciones principales

### 1. Conversión de formatos (Data Translation):

Adapta los datos entre diferentes esquemas de codificación, como **ASCII ↔ Unicode** o **EBCDIC ↔ ASCII**, para garantizar compatibilidad entre plataformas.

### 2. Compresión y descompresión:

Reduce el tamaño de los datos transmitidos para optimizar el rendimiento y disminuir el tiempo de envío.

- Ejemplo: compresión de imágenes (JPEG) o vídeo (MPEG).

### 3. Cifrado y descifrado:

Protege la privacidad y la integridad de los datos en tránsito.

- Ejemplo: **TLS/SSL**, usados en HTTPS, cifran los datos antes de enviarlos.

#### 4. Formateo de estructuras complejas:

Establece reglas para datos multimedia, texto, imágenes o audio, garantizando su correcta interpretación.

### ◆ Protocolos, estándares y formatos asociados

Categoría	Ejemplos	Descripción
Codificación de texto	ASCII, EBCDIC, Unicode	Define cómo se representan caracteres en binario.
Formatos multimedia	JPEG, GIF, MPEG, PNG	Especifica compresión y estructura visual.
Cifrado / Seguridad	SSL, TLS	Garantizan confidencialidad e integridad.
Intercambio de datos	XML, JSON	Formatos estándar para comunicación estructurada.

 Esta capa convierte los datos de aplicación en un formato que las capas inferiores pueden manejar sin perder su significado.

### ◆ Ejemplo práctico

Cuando un usuario accede a un sitio web HTTPS:

1. La capa 6 en el navegador cifra los datos usando **TLS** antes de enviarlos.
2. El servidor web descifra los datos en su propia capa de presentación.
3. Ambos usan el mismo método de compresión y codificación para interpretar el contenido HTML correctamente.

## 10 Session Layer (Capa 5)

La **Session Layer** coordina y administra la **comunicación continua entre dos sistemas**.

Define cómo se crean, mantienen y finalizan las sesiones, garantizando que los intercambios de datos se realicen de manera ordenada.

 Mientras la capa 4 transporta los datos, la capa 5 organiza el “diálogo” entre aplicaciones.

### ◆ Funciones principales

#### 1. Establecimiento, mantenimiento y terminación de sesiones:

Crea una conexión lógica entre los procesos en los sistemas origen y destino.

Gestiona el inicio, duración y cierre de la sesión (por ejemplo, sesión SSH o de base de datos).

#### 2. Sincronización:

Coloca **checkpoints** o marcadores de sincronización durante una transmisión larga.

Si la conexión se interrumpe, la sesión puede reanudarse desde el último punto verificado.

- Ejemplo: en una descarga de archivo grande, la sesión puede reiniciarse sin repetir todo el proceso.

#### 3. Control de diálogo:

Define el **modo de comunicación**:

- **Simplex**: transmisión en una sola dirección.
- **Half-duplex**: ambas direcciones, pero no simultáneamente.

- **Full-duplex:** transmisión simultánea en ambas direcciones.

#### 4. Separación de flujos (Session Multiplexing):

Permite que un mismo dispositivo mantenga **múltiples sesiones independientes**.

- Ejemplo: un navegador con varias pestañas conectadas a diferentes servidores web.

### ◆ Protocolos y ejemplos

Protocolo	Descripción
NetBIOS / NetBEUI	Gestiona sesiones y nombres de red en sistemas Windows antiguos.
PPTP / L2TP	Establecen y mantienen túneles VPN.
RPC (Remote Procedure Call)	Permite ejecutar funciones en sistemas remotos.
SQL Sessions / NFS	Mantienen conexiones persistentes para intercambio de datos.

 La capa de sesión mantiene la lógica de la conversación: quién habla, cuándo y durante cuánto tiempo.

### ◆ Ejemplo práctico

En una conexión **telnet** o **SSH**:

1. El cliente inicia sesión con el servidor (autenticación).
2. Se establece un canal de comunicación full-duplex.
3. Si la conexión se interrumpe, la sesión puede reiniciarse desde el punto anterior.
4. Cuando el usuario sale, la sesión se cierra limpiamente.

### ◆ Relación entre las capas superiores

Capa	Enfoque	Ejemplo de función
7 – Application	Interacción con el usuario / servicios	HTTP, FTP, SMTP
6 – Presentation	Formato, cifrado y compresión	TLS, JPEG, ASCII
5 – Session	Control del diálogo / sincronización	RPC, NetBIOS, PPTP

 Las capas superiores no se ocupan del transporte físico de datos, sino de la lógica, formato y control de la comunicación entre aplicaciones.

## 11 Transport Layer (Capa 4)

La **Transport Layer** gestiona el **transporte confiable de datos** entre sistemas finales.

Divide los datos en **segmentos**, controla el flujo, corrige errores y garantiza la **entrega ordenada**.

**Funciones principales:**

1. **Segmentación y reensamblaje:** los datos de la capa superior se dividen en unidades más pequeñas (segmentos).
2. **Establecimiento de conexión lógica** entre los dispositivos emisores y receptores.
3. **Corrección de errores:** detecta y reenvía datos perdidos o dañados.
4. **Control de flujo:** ajusta la velocidad de transmisión para evitar congestión.

5. **Multiplexación:** permite que varias aplicaciones comparten una misma conexión física.

### Protocolos utilizados:

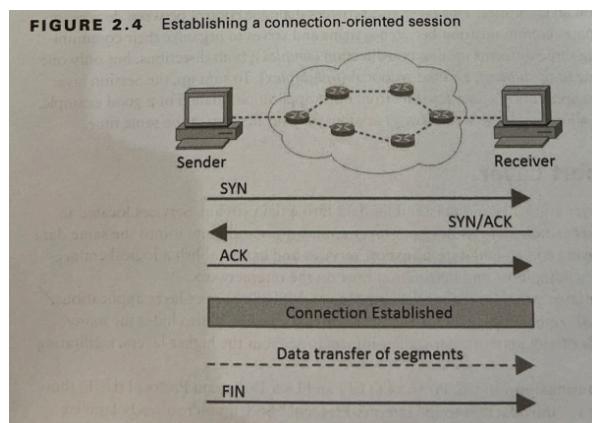
Protocolo	Tipo de servicio	Características principales
<b>TCP (Transmission Control Protocol)</b>	Orientado a conexión	Fiable, usa confirmaciones (ACK), reenvíos y control de flujo.
<b>UDP (User Datagram Protocol)</b>	No orientado a conexión	Rápido, sin control de errores, ideal para streaming o VoIP.

 TCP prioriza la fiabilidad; UDP, la velocidad.

## ◆ Comunicación orientada a conexión (TCP)

TCP utiliza un proceso llamado **Three-Way Handshake** para establecer una conexión confiable entre dos dispositivos.

Paso	Descripción
SYN	El cliente solicita la conexión.
SYN/ACK	El servidor confirma y responde.
ACK	El cliente confirma y la conexión queda establecida.



Una vez establecida, los datos fluyen en ambas direcciones.

Durante la transmisión, cada segmento recibido se **confirma** con un mensaje **ACK**.

Si el ACK no llega dentro de un tiempo límite, el segmento se **retransmite**.

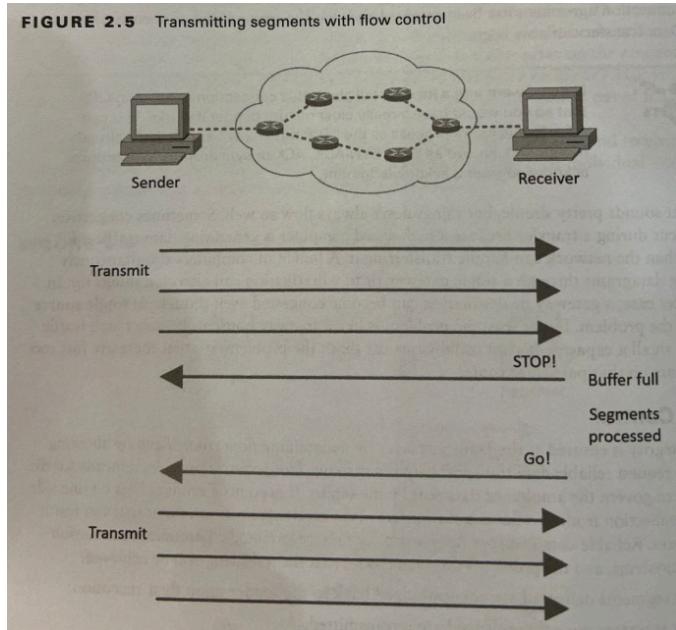
## ◆ Control flow

Evita que un emisor rápido **sature** a un receptor más lento.

Cuando el receptor detecta que su **buffer** está lleno, envía una señal **Stop/Go**:

1. El emisor detiene la transmisión ("Stop").
2. Cuando el receptor procesa los datos, envía una señal "Go" para continuar.

**FIGURE 2.5** Transmitting segments with flow control



De este modo se asegura una comunicación ordenada y sin pérdidas.

## ◆ Windowing

El **windowing** mejora la eficiencia al permitir enviar varios segmentos antes de recibir confirmaciones. El tamaño de la ventana (window size) define cuántos bytes pueden transmitirse sin esperar un **ACK** (Acknowledgment).

### Ejemplo:

- **Ventana = 1:** el emisor espera un ACK por cada segmento.
- **Ventana = 3:** puede enviar tres segmentos seguidos antes de esperar confirmación.

Si el receptor pierde datos o detecta errores, **reduce el tamaño de la ventana** para estabilizar la conexión.

| *Este mecanismo optimiza el rendimiento del TCP al equilibrar velocidad y fiabilidad.*

## ✉ ACK (Acknowledgment)

**ACK** es la abreviatura de **Acknowledgment**, que significa **confirmación de recepción**.

Forma parte del mecanismo de control de errores del protocolo **TCP** (capa 4 del modelo OSI).

### ◆ Función principal

Cuando un dispositivo **recibe correctamente un segmento TCP**, envía un mensaje **ACK** al emisor indicando que los datos llegaron de forma íntegra.

Esto permite que el emisor sepa **qué información fue recibida con éxito** y pueda continuar enviando nuevos segmentos.

### ◆ Flujo del proceso

1. El **emisor** envía uno o varios segmentos numerados.
2. El **receptor** verifica la integridad y el orden de los segmentos.
3. Si todo está correcto, responde con un **ACK** que incluye el **número de secuencia esperado** para el siguiente segmento.

4. Si falta un segmento o hay error, **no se envía el ACK**, lo que obliga al emisor a retransmitir los datos perdidos.

## ◆ Ejemplo práctico

Paso	Acción	Descripción
1	Emisor envía <b>Segmento 1 (Seq=1000)</b>	Contiene datos iniciales.
2	Receptor recibe correctamente el segmento	Envía <b>ACK=1001</b> , indicando que espera el byte siguiente.
3	Emisor envía <b>Segmento 2 (Seq=1001)</b>	Continua la transmisión.
4	Si el receptor no envía ACK	El emisor asume pérdida y retransmite el segmento.

 Cada ACK confirma la recepción hasta un número de secuencia específico. Los ACK acumulativos permiten confirmar varios segmentos a la vez.

## ◆ Relación con el Windowing

El **windowing** y los **ACK** trabajan conjuntamente:

- La **ventana TCP (window size)** determina cuántos datos pueden enviarse sin esperar un ACK.
- Los **ACK** marcan el ritmo de la transmisión, ya que confirman qué parte del flujo ha sido recibida y cuál puede enviarse a continuación.

 Cuantos más ACK se reciben sin errores, más puede crecer la ventana, mejorando el rendimiento y la velocidad.

## 1 2 Conclusión de las capas superiores

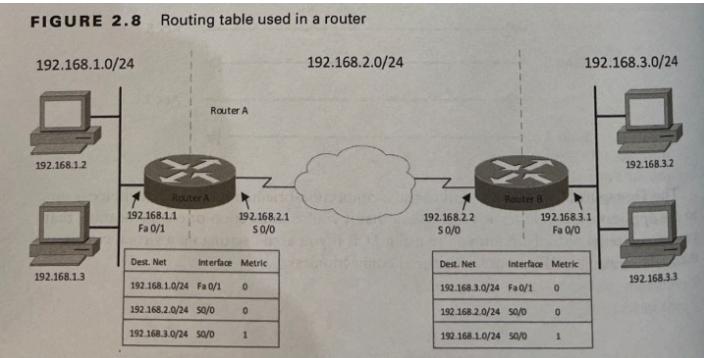
Capa	Función principal	Protocolos / Ejemplos
7 – Application	Interacción directa con el usuario y servicios de red	HTTP, FTP, DNS, SMTP
6 – Presentation	Traducción, compresión y cifrado de datos	TLS, SSL, JPEG, ASCII
5 – Session	Establecimiento y control de sesiones entre aplicaciones	NetBIOS, RPC
4 – Transport	Entrega confiable, control de flujo y corrección de errores	TCP, UDP

## 1 3 Network Layer (Capa 3)

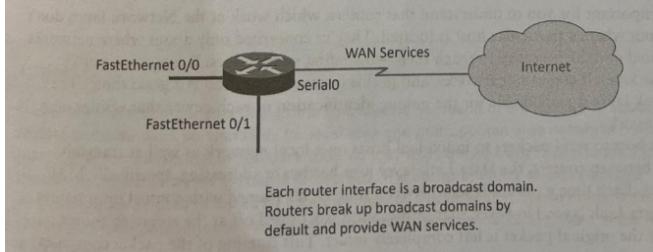
La **Network Layer** se encarga de **mover los paquetes de datos desde el origen hasta el destino** a través de múltiples redes interconectadas (internetwork).

Su función principal es proporcionar **conectividad entre redes diferentes** y determinar la **mejor ruta disponible** para cada paquete.

**FIGURE 2.8** Routing table used in a router



**FIGURE 2.9** A router in an internetwork



🌐 En esta capa, los datos dejan de ser locales (LAN) y se transforman en tráfico enrutable que puede viajar a cualquier parte de la red.

## ◆ Funciones principales

### 1. Direccionamiento lógico:

Cada dispositivo recibe una **dirección IP única** (IPv4 o IPv6).

Estas direcciones permiten identificar la ubicación de origen y destino de los paquetes en la red.

- Se componen de dos partes: **Network ID** (identifica la red) y **Host ID** (identifica el dispositivo).
- A diferencia de las direcciones MAC, las IP **pueden cambiar** si el dispositivo se conecta a otra red.

### 2. Encapsulación:

La capa de red recibe los **segmentos TCP** o **datagramas UDP** desde la capa de transporte y los encapsula en **paquetes IP** (también llamados **datagramas**).

- Cada paquete incluye direcciones IP de **origen** y **destino**, además de otros campos de control.
- Este proceso también puede incluir fragmentación, si el paquete supera el tamaño máximo permitido por el medio.

### 3. Fragmentación y reensamblaje:

Cuando un paquete excede la **MTU (Maximum Transmission Unit)** de una red intermedia, se **divide en fragmentos**.

- Cada fragmento lleva su propio encabezado IP y un campo que indica su posición en el paquete original.
- El **reensamblaje** se realiza en el **host de destino**, nunca en routers intermedios.
- Ejemplo: un paquete IP de 2000 bytes que pasa por una red con MTU de 1500 bytes será dividido en dos fragmentos.

### 4. Enrutamiento (Routing):

La capa 3 determina la **mejor ruta** que debe seguir cada paquete.

Esto puede realizarse de forma **estática** (configurada manualmente) o **dinámica** (mediante protocolos de enrutamiento).

- **Static routing:** el administrador configura manualmente las rutas; útil en redes pequeñas y estables.

- **Dynamic routing:** los routers intercambian información de rutas automáticamente usando protocolos como **OSPF, EIGRP, RIP, BGP**.
- Los routers mantienen **tablas de enrutamiento** con redes conocidas y las métricas asociadas (distancia, coste, número de saltos, ancho de banda, etc.).

## 5. Control de congestión:

Cuando una red intermedia se satura, los routers pueden descartar paquetes o marcar mensajes **ICMP Source Quench** (deprecated pero útil conceptualmente) para informar al emisor que **reduzca la velocidad de transmisión**.

Este proceso ayuda a **mantener la estabilidad del tráfico**.

## 6. Selección de ruta (Path Determination):

La capa de red usa **métricas** para elegir la ruta más eficiente. Entre las métricas comunes se incluyen:

- **Hop count:** número de routers intermedios.
- **Bandwidth:** capacidad del enlace.
- **Delay:** tiempo de tránsito del paquete.
- **Cost:** valor asignado por el administrador.
- **Load:** nivel de tráfico en la ruta.

## ◆ Estructura del paquete IP

Cada **paquete IP (IPv4)** tiene un encabezado con información crítica para el enrutamiento:

Campo	Función
<b>Version</b>	Indica si es IPv4 o IPv6.
<b>Header Length</b>	Tamaño del encabezado.
<b>Type of Service (ToS)</b>	Define prioridad o calidad de servicio (QoS).
<b>Total Length</b>	Longitud total del paquete (datos + encabezado).
<b>Identification, Flags, Fragment Offset</b>	Controlan la fragmentación.
<b>Time to Live (TTL)</b>	Número máximo de saltos antes de que el paquete sea descartado.
<b>Protocol</b>	Identifica si el contenido pertenece a TCP, UDP, ICMP, etc.
<b>Header Checksum</b>	Verifica la integridad del encabezado.
<b>Source Address / Destination Address</b>	Direcciones IP de origen y destino.

💡 Cada vez que un paquete pasa por un router, el valor **TTL** se reduce en 1. Si llega a cero, el router descarta el paquete y envía un mensaje ICMP "Time Exceeded" al emisor.

## ◆ Protocolos de la Capa 3

Tipo	Ejemplo	Función
Protocolo de red	<b>IP (Internet Protocol)</b>	Proporciona direccionamiento lógico y enrutamiento de paquetes.
Protocolo de control	<b>ICMP (Internet Control Message Protocol)</b>	Diagnóstico y notificación de errores.

Tipo	Ejemplo	Función
Protocolo de seguridad	IPsec (Internet Protocol Security)	Cifra y autentica la comunicación IP.
Protocolo de descubrimiento	ARP (Address Resolution Protocol) y NDP (Neighbor Discovery Protocol)	Traduce direcciones IP ↔ MAC.

## ◆ ICMP (Internet Control Message Protocol)

**ICMP** es esencial para el control y la notificación de errores en redes IP.

Se utiliza para enviar mensajes de control y diagnóstico, **no para transportar datos de usuario**.

**Ejemplos de mensajes ICMP:**

- Echo Request / Echo Reply → usados por **ping** para probar conectividad.
- Destination Unreachable → indica que un destino no es accesible.
- Time Exceeded → TTL agotado (utilizado por **traceroute**).
- Redirect → sugiere una mejor ruta.

 *ICMP opera en la capa 3, pero los mensajes se encapsulan dentro de paquetes IP estándar.*

## ◆ Dispositivos y componentes de la Capa 3

Dispositivo	Función
Router	Encaminamiento de paquetes entre redes distintas. Mantiene tablas de rutas.
Multilayer Switch	Combina funciones de switch (capa 2) y router (capa 3).
Firewall de capa 3	Filtrar tráfico en función de direcciones IP, protocolos o puertos.
Gateway	Traduce protocolos entre redes con arquitecturas diferentes.

## ◆ Relación entre la Capa 3 y otras capas

- **Con la capa 4 (Transport):** recibe los **segmentos TCP/UDP** y les agrega información de direccionamiento IP.
- **Con la capa 2 (Data Link):** entrega los **paquetes IP** para ser encapsulados en **frames Ethernet, PPP, o HDLC** antes de su envío físico.

 *Cada salto (router) desencapsula el frame, inspecciona el paquete IP y lo vuelve a encapsular antes de reenviarlo.*

## ◆ Resumen visual

Proceso de transmisión de un paquete a través de redes:

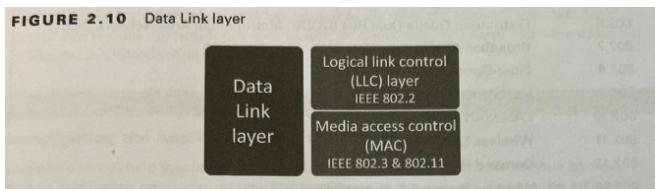
- 1 La aplicación envía datos → capa 4 los segmenta.
- 2 La capa 3 encapsula los segmentos en **paquetes IP** y decide la ruta.
- 3 Cada router examina la dirección de destino, **actualiza el TTL**, y reenvía el paquete.
- 4 Al llegar al destino, la capa 3 lo entrega a la capa 4 para su reensamblaje.

 La Network Layer es el “motor de la red”: sin ella no habría conectividad entre redes ni posibilidad de Internet tal como la conocemos.

## 1 4 Data Link Layer (Capa 2)

La **Data Link Layer** proporciona un método confiable para **transferir datos a través de un enlace físico** dentro de una red local (LAN o WAN).

Su principal función es **garantizar la entrega libre de errores** entre dispositivos directamente conectados y **controlar el acceso al medio compartido**.



 Si la capa física transmite bits, la capa de enlace de datos les da sentido estructural en forma de tramas (frames).

### ◆ Funciones principales

#### 1. Encapsulación en tramas (framing):

Los datos de la capa 3 (paquetes IP) se encapsulan en **frames**, que incluyen un encabezado y un tráiler.

- El **encabezado** contiene direcciones MAC y control de flujo.
- El **tráiler** incluye el campo **FCS (Frame Check Sequence)** para verificar errores.

#### 2. Direccionamiento físico:

Cada dispositivo de red posee una dirección **MAC (Media Access Control)** única grabada en su tarjeta de red (NIC).

- Se representa en formato hexadecimal de 48 bits ( 00:1A:2B:3C:4D:5E ).
- Permite que los dispositivos se identifiquen dentro del mismo segmento de red.

#### 3. Detección y control de errores:

- Mediante **FCS (Frame Check Sequence)**, el receptor puede detectar si un frame ha sido alterado durante la transmisión.
- Si se detecta error, la trama se descarta y el nivel superior (TCP en la capa 4) gestionará la retransmisión.

#### 4. Control de acceso al medio (MAC):

La capa 2 define **cómo y cuándo los dispositivos pueden acceder al medio físico** para enviar datos, evitando colisiones o interferencias.

- En redes Ethernet se utiliza **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**.
- En redes inalámbricas (Wi-Fi), el método es **CSMA/CA (Collision Avoidance)**.

#### 5. Sincronización de tramas:

Los encabezados incluyen **campos de delimitación** (Start Frame Delimiter) que indican cuándo comienza una trama.

Esto asegura que el receptor interprete los bits en el orden correcto.

## ◆ Subcapas de la Capa 2

La **Data Link Layer** se divide en dos subcapas definidas por el estándar **IEEE 802**:

Subcapa	Función principal
<b>LLC (Logical Link Control)</b>	Controla la comunicación entre dispositivos. Identifica qué protocolo de capa 3 (IP, IPX, ARP) se está utilizando. Añade control de flujo y multiplexación.
<b>MAC (Media Access Control)</b>	Gestiona el acceso al medio físico (Ethernet, Wi-Fi, etc.) y contiene las direcciones físicas (MAC). Determina cuándo un dispositivo puede transmitir.

 La subcapa LLC interactúa con la capa 3, mientras que la MAC se comunica directamente con la capa física.

## ◆ Estructura de una trama Ethernet (Frame)

Campo	Tamaño (bytes)	Descripción
Preamble + SFD	8	Sincroniza transmisor y receptor.
Destination MAC Address	6	Dirección del dispositivo destino.
Source MAC Address	6	Dirección del dispositivo origen.
Type/Length	2	Indica el protocolo de capa 3 (ej. IPv4 = 0x0800).
Data (Payload)	46–1500	Contiene el paquete IP u otros datos.
FCS (Frame Check Sequence)	4	Campo de verificación de errores (CRC).

 El tamaño máximo de un frame Ethernet estándar es de 1518 bytes (MTU = 1500 bytes para datos).

## ◆ Funcionamiento de CSMA/CD (Ethernet cableada)

**CSMA/CD** regula cómo los dispositivos comparten el medio para evitar colisiones en entornos de red tradicionales (por ejemplo, con hubs).

1. **Carrier Sense:** cada dispositivo “escucha” el medio antes de transmitir.
2. **Multiple Access:** varios dispositivos pueden detectar si el canal está libre.
3. **Collision Detection:** si dos dispositivos transmiten al mismo tiempo, se detecta una colisión.
4. **Retransmisión aleatoria:** los dispositivos esperan un tiempo aleatorio (backoff) antes de reintentar.

 En redes modernas con **switches full-duplex**, el CSMA/CD ya no es necesario, ya que no existen colisiones.

## ◆ Funcionamiento de CSMA/CA (Ethernet inalámbrica)

En Wi-Fi (IEEE 802.11), se utiliza **CSMA/CA (Collision Avoidance)**:

- Los dispositivos anuncian su intención de transmitir mediante tramas de **Request to Send (RTS)** y **Clear to Send (CTS)**.
- Esto minimiza la posibilidad de colisiones en medios no compartidos físicamente.

## ◆ Protocolos y tecnologías de la Capa 2

Categoría	Ejemplo	Descripción
LAN	Ethernet (IEEE 802.3)	Tecnología más común en redes cableadas.
WLAN	Wi-Fi (IEEE 802.11)	Red inalámbrica local.
WAN	PPP, HDLC, Frame Relay	Protocolos punto a punto usados en enlaces dedicados.
Virtual LAN	VLAN (IEEE 802.1Q)	Permite segmentar lógicamente una red en dominios independientes.

Standard	Topic
802.1	LAN/MAN Management (and Media Access Control Bridges)
802.2	Logical Link Control
802.3	CSMA/CD (Ethernet)
802.4	Token Passing Bus
802.5	Token Passing Ring
802.6	Distributed Queue Dual Bus (DQDB) Metropolitan Area Network (MAN)
802.7	Broadband Local Area Networks
802.8	Fiber-Optic LANs and MANs
802.9	Isochronous LANs
802.10	LAN/MAN Security
802.11	Wireless LAN
802.12	Demand Priority Access Method
802.15	Wireless Personal Area Network
802.16	Wireless Metropolitan Area Network (also called WiMAX)
802.17	Resilient Packet Ring

Note that 802.1, 802.3, 802.11, and 802.15 are the only Active 802 standards. The others are either Disbanded or Hibernating.

The takeaway is to remember that 802.3 calls out anything having to do with Ethernet, and 802.11 is anything wireless.

La imagen muestra una **tabla del libro Network+ Study Guide (N10-009)** sobre los estándares IEEE 802, que forman parte del **Project 802** desarrollado por el **IEEE (Institute of Electrical and Electronics Engineers)**.

Este proyecto define las normas utilizadas en la **Data Link Layer (Capa 2)** del modelo OSI y, en algunos casos, en la capa física.

## Project 802 — IEEE LAN/MAN Standards

El **Project 802** se creó en **1980** para establecer un marco común para las **redes locales (LAN)** y **redes metropolitanas (MAN)**.

El nombre “802” proviene del año (1980) y del mes (febrero) en que se inició el comité.

Cada subcomité 802 define un **protocolo o tecnología de red**.

Las normas activas se actualizan periódicamente y muchas se han convertido en la base de las redes actuales.

## Tabla resumen

Standard IEEE	Tema principal
802.1	LAN/MAN Management y control de puentes MAC
802.2	Logical Link Control (LLC)
802.3	CSMA/CD (Ethernet)
802.4	Token Passing Bus
802.5	Token Passing Ring
802.6	DQDB Metropolitan Area Network (MAN)
802.7	Broadband LANs

Standard IEEE	Tema principal
802.8	Fiber-Optic LANs y MANs
802.9	Isochronous LANs
802.10	LAN/MAN Security
802.11	Wireless LAN (Wi-Fi)
802.12	Demand Priority Access Method
802.15	Wireless Personal Area Network (Bluetooth, ZigBee)
802.16	Wireless Metropolitan Area Network (WiMAX)
802.17	Resilient Packet Ring

## 🔍 Notas importantes (según el texto del libro)

- Los únicos estándares **activos** actualmente son **802.1, 802.3, 802.11 y 802.15**. Los demás están **en desuso (disbanded o hibernating)**.
- 802.3** → **Ethernet**: todo lo relacionado con redes cableadas LAN.
- 802.11** → **Wireless**: todo lo relacionado con Wi-Fi.
- 802.15** → **WPAN**: Bluetooth y redes personales inalámbricas.
- 802.1** → **Control y gestión de red**, incluyendo VLANs y bridges.

### 💡 Idea clave:

El Project 802 proporciona la base técnica de las redes modernas.

En resumen:

- 802.3** → **Ethernet (cableado)**
- 802.11** → **Wireless LAN (Wi-Fi)**
- 802.15** → **Personal networks (Bluetooth)**
- 802.1** → **Control y seguridad de red (VLAN, QoS, STP)**

## ◆ Dispositivos que operan en Capa 2

Dispositivo	Función
Switch	Reenvía tramas dentro de la LAN según las direcciones MAC.
Bridge	Divide una red en segmentos para reducir colisiones.
NIC (Network Interface Card)	Interfaz física que encapsula y desencapsula tramas.
Access Point (modo bridge)	Enlaza clientes inalámbricos con la red cableada.

## ◆ Tablas MAC y aprendizaje dinámico

Los **switches** mantienen una **tabla CAM (Content Addressable Memory)** con las direcciones MAC asociadas a cada puerto.

### Proceso de aprendizaje:

1. Cuando un switch recibe una trama, lee la **dirección MAC de origen**.
2. La almacena junto con el **puerto de entrada** en su tabla MAC.
3. Para reenviar, busca la **dirección MAC de destino**:

- Si está en la tabla, envía la trama solo por ese puerto (unicast).
- Si no está, la **inunda (flood)** por todos los puertos (excepto el de origen).

 Este mecanismo hace que los switches sean más eficientes que los hubs, reduciendo el tráfico innecesario.

## ◆ Errores y control de flujo

- **Errores detectados:** bit corrupto, colisión o pérdida de sincronización.
- **Mecanismo de detección:** FCS usa un cálculo de **CRC (Cyclic Redundancy Check)** para comparar resultados entre emisor y receptor.
- **Corrección:** la capa 2 solo detecta, no corrige; la retransmisión la gestiona TCP (capa 4).

## ◆ Resumen visual

+-----+	
Layer 2: Data Link	
+-----+	
- Framing	
- MAC addressing	
- Error detection (FCS)	
- Flow & access control	
- LLC/MAC sublayers	
+-----+	

 La Capa 2 actúa como un “traductor físico-lógico”: toma paquetes IP de la capa 3, los encapsula en tramas y los entrega al medio físico (Capa 1).

## 1 | 5 Physical Layer (Capa 1)

La **Physical Layer** es la base del modelo OSI.

Define las **características eléctricas, mecánicas, funcionales y procedimentales** necesarias para la transmisión física de bits entre dispositivos.

Su misión es convertir la información digital en **señales físicas** (eléctricas, ópticas o de radio) que puedan viajar a través del medio de comunicación.

 Esta capa no entiende direcciones ni protocolos; su única función es mover bits de un punto a otro.

## ◆ Funciones principales

### 1. Transmisión y recepción de bits:

- Convierte datos binarios (1 y 0) en señales eléctricas, luminosas o de radiofrecuencia.
- A la inversa, convierte las señales recibidas de nuevo en datos digitales interpretables.

### 2. Definición de medios físicos:

- Especifica los tipos de cables, conectores, longitudes máximas, topologías y niveles de voltaje.
- Ejemplos: cobre (UTP/STP), fibra óptica, radiofrecuencia (Wi-Fi, Bluetooth).

### 3. Codificación de señales (Encoding):

- Determina cómo los bits se representan en forma de señal.
- Ejemplos:
  - **NRZ (Non-Return-to-Zero)**: 1 y 0 se representan por niveles de voltaje distintos.
  - **Manchester**: la transición de nivel indica el bit transmitido.
  - **8B/10B**: usa 10 bits para codificar 8 bits de datos (Ethernet Gigabit).

#### 4. Modulación:

- Proceso mediante el cual una señal digital se combina con una **portadora analógica** para su envío.
- Métodos comunes:
  - **AM (Amplitude Modulation)** – cambia la amplitud según los datos.
  - **FM (Frequency Modulation)** – la frecuencia varía con los bits.
  - **PSK (Phase Shift Keying)** – cambia la fase de la onda portadora.
  - **QAM (Quadrature Amplitude Modulation)** – combina amplitud y fase (Wi-Fi y DOCSIS).

#### 5. Sincronización:

- Asegura que transmisor y receptor interpreten los bits al mismo ritmo de reloj (clock).
- Puede lograrse mediante señales de sincronización o codificaciones autosincronizables (Manchester).

#### 6. Topología física:

- Define la **disposición real** de los dispositivos en la red.
- Ejemplos: **estrella, bus, anillo, malla y punto a punto**.

### ◆ Medios físicos más comunes

Medio	Descripción	Características principales
Cobre (UTP/STP)	Pares trenzados con conectores <b>RJ-45</b> .	Económico, fácil de instalar, limitado a 100 m.
Cable coaxial	Núcleo de cobre rodeado de aislamiento y malla metálica.	Alta inmunidad a interferencias; usado en redes legacy y DOCSIS.
Fibra óptica	Señales de luz por filamento de vidrio o plástico.	Gran velocidad y distancia; inmune a EMI.
Inalámbrico (RF)	Transmisión por ondas de radio o microondas.	Flexible y móvil; susceptible a interferencias.

### ◆ Dispositivos de la Capa 1

Dispositivo	Función
Hubs	Repiten señales a todos los puertos; no filtran ni interpretan datos.
Repeaters	Regeneran y amplifican señales para extender la distancia.
Media converters	Transforman un medio en otro (p. ej. cobre ↔ fibra).
Transceivers (SFP, GBIC)	Módulos ópticos o eléctricos usados en switches / routers.
Cables y conectores	Elementos físicos de transmisión: RJ-45, LC, SC, ST, BNC.

 A diferencia de las capas superiores, la capa física no toma decisiones lógicas.

## ◆ Parámetros físicos importantes

Parámetro	Definición	Ejemplo
<b>Bandwidth</b>	Capacidad máxima de datos por segundo.	1 Gbps, 10 Gbps
<b>Throughput</b>	Rendimiento real percibido.	≈ 950 Mbps en Gigabit Ethernet
<b>Latency</b>	Tiempo de ida de un bit.	< 5 ms en LAN
<b>Attenuation</b>	Pérdida de potencia de la señal.	Se corrige con repetidores o fibra.
<b>Noise</b>	Interferencias externas.	EMI, RFI

## ◆ Codificación y modulación

### Codificación digital (line coding):

Define cómo se representan los bits en voltaje, luz o frecuencia.

Ejemplo (Manchester 10BASE-T):

- Transición alta → baja = 1
- Transición baja → alta = 0

Ventaja: autosincronizable y tolerante a errores de reloj.

### Modulación digital:

Usada en redes inalámbricas y de larga distancia.

- **ASK, FSK, PSK, QAM** permiten enviar información digital por medios analógicos.

 La modulación convierte señales baseband en passband, adecuadas para transmisión física.

## ◆ Topologías físicas más comunes

Tipo	Descripción	Uso típico
<b>Estrella (Star)</b>	Todos los nodos se conectan a un dispositivo central.	LAN modernas.
<b>Bus</b>	Un solo cable compartido.	Ethernet legacy.
<b>Anillo (Ring)</b>	Nodos conectados en circuito cerrado.	Token Ring, FDDI.
<b>Malla (Mesh)</b>	Conexiones redundantes entre nodos.	Backbones y enlaces WAN.
<b>Punto a punto (P2P)</b>	Enlace directo entre dos dispositivos.	Conexiones seriales WAN.

## ◆ Relación con las capas superiores

- Recibe **tramas** desde la capa 2 y las convierte en señales físicas.
- Entrega señales recibidas a la capa 2 para reensamblarlas.
- No ofrece control de errores ni flujo; eso pertenece a la Data Link Layer.

## ◆ Resumen visual

Layer 1: Physical
- Señales eléctricas/ópticas
- Cables y conectores
- Codificación y modulación
- Topologías físicas
- Dispositivos: hubs, repeaters

## ◆ Introduction to Encapsulation

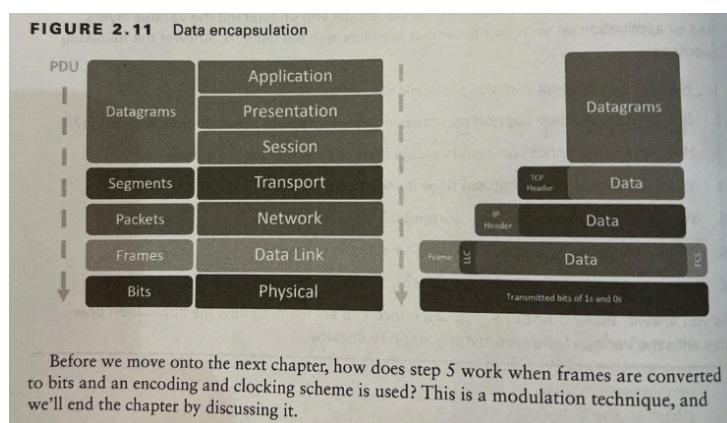
Cuando un host transmite datos a otro, cada capa del modelo OSI **agrega su propia información de control** al conjunto de datos.

Este proceso se llama **encapsulation** y produce unidades denominadas **Protocol Data Units (PDUs)**.

 Cada capa se comunica con su par en el host remoto utilizando su propio encabezado o tráiler.

## ◆ Proceso de encapsulación paso a paso

1. **La Application Layer** convierte la información del usuario en datos listos para transmisión.
2. **La Transport Layer** divide los datos en **segmentos** y establece una conexión fiable entre los hosts.
3. **La Network Layer** encapsula los segmentos en **paquetes o datagramas**, agregando direcciones IP.
4. **La Data Link Layer** encapsula los paquetes en **frames**, añadiendo direcciones MAC para la red local.
5. **La Physical Layer** convierte las tramas en **bits** que se envían por el medio físico.



Cada capa agrega su propio encabezado (y a veces tráiler) formando una cadena jerárquica de encapsulación.

## ◆ PDUs por capa

Capa OSI	Unidad de datos	Encabezado principal
Application / Presentation / Session	Datos	Información de aplicación
Transport	Segmento	Números de puerto, secuenciación
Network	Paquete / Datagrama	Direcciones IP
Data Link	Frame	Direcciones MAC + CRC
Physical	Bits	Señal eléctrica / óptica / radio

 En recepción, el proceso se invierte: cada capa elimina su encabezado (decapsulation).

## ◆ Exercise 2.1 — Investigating the Applications and the OSI Model

Ejercicio propuesto en el libro para analizar cómo una aplicación interactúa con las distintas capas del modelo OSI.

El objetivo es identificar qué función cumple cada capa cuando una aplicación accede a la red, desde la interacción del usuario hasta la transmisión física de los bits.

Pregunta	Respuesta / Explicación detallada
<b>1. How do you interact with the application?</b>	A través de una <b>interfaz de usuario</b> (GUI o CLI). Por ejemplo, un navegador web, un cliente de correo o una app FTP permiten al usuario introducir datos y recibir respuestas. Esta interacción ocurre en la <b>Application Layer (Capa 7)</b> , que proporciona los servicios y protocolos que usan las aplicaciones para comunicarse (HTTP, SMTP, DNS, etc.).
<b>2. Does the application support compression or encryption?</b>	Si la aplicación utiliza <b>cifrado (TLS/SSL)</b> para proteger la comunicación o <b>compresión (ZIP, MPEG, GZIP)</b> para optimizar el envío de datos, estas funciones se gestionan en la <b>Presentation Layer (Capa 6)</b> . Por ejemplo, HTTPS cifra los datos antes de enviarlos, y un vídeo en streaming puede comprimir su contenido en formato H.264 o MPEG.
<b>3. How does the application communicate (half-duplex, full-duplex, simplex)?</b>	El tipo de comunicación (una dirección, alternada o simultánea) lo controla la <b>Session Layer (Capa 5)</b> . Por ejemplo, una videollamada VoIP usa <b>full-duplex</b> para permitir audio bidireccional simultáneo, mientras que un altavoz Bluetooth podría operar en <b>half-duplex</b> (envío o recepción, pero no ambos a la vez).
<b>4. Which Transport layer protocol does it use to communicate?</b>	Las aplicaciones utilizan <b>TCP</b> o <b>UDP</b> según el nivel de fiabilidad requerido. Por ejemplo: <b>HTTP, HTTPS, FTP y SMTP</b> usan <b>TCP</b> (orientado a conexión y con confirmación de entrega), mientras que <b>DNS, DHCP o VoIP</b> usan <b>UDP</b> (sin conexión, más rápido pero sin garantía de entrega). Esta función pertenece a la <b>Transport Layer (Capa 4)</b> .
<b>5. What is the IP address of your computer?</b>	La <b>Network Layer (Capa 3)</b> se encarga de asignar direcciones lógicas (IPv4 o IPv6) para identificar el origen y destino de los paquetes. Por ejemplo, una computadora con IP 192.168.1.10 puede comunicarse con un servidor web remoto en 142.250.190.14 (Google). Aquí actúan protocolos como <b>IP, ICMP o IPsec</b> .
<b>6. What method of connectivity do you have to the network?</b>	La <b>Data Link Layer (Capa 2)</b> define cómo se transmite la información entre dispositivos dentro de la misma red local. Determina si la conexión es <b>Ethernet (cableada)</b> o <b>Wi-Fi (inalámbrica)</b> , usa <b>direcciones MAC</b> para identificar dispositivos y controla errores mediante <b>frames</b> . Ejemplo: tarjeta de red Ethernet con MAC 00:1A:2B:3C:4D:5E .
<b>7. Is it connected with wired or wireless media?</b>	Esta es función de la <b>Physical Layer (Capa 1)</b> , que especifica el medio físico de transmisión (cables de cobre, fibra óptica o señales de radio). Si estás conectado por cable RJ-45, usas Ethernet; si es mediante una antena Wi-Fi o Bluetooth, el medio es inalámbrico. La capa física transmite los bits mediante señales eléctricas, ópticas o electromagnéticas.

 Este ejercicio demuestra cómo una simple acción —como abrir una página web— implica la intervención coordinada de todas las capas del modelo OSI, desde la solicitud HTTP en la capa 7 hasta

la transmisión de bits en la capa 1.

## ◆ Modulation Techniques

La **modulación** transforma una señal digital (baseband) en una **passband signal** capaz de viajar por un canal físico analógico.

Permite transmitir datos a través de diferentes medios como cobre, fibra o aire.

## ◆ Conceptos clave

- **Baseband signal:** señal digital que usa todo el ancho de banda del canal.  
Ejemplo: Ethernet 10BASE-T.
- **Passband signal:** señal modulada en una portadora analógica, necesaria para transmisión inalámbrica o de larga distancia.

**Modem** = *modulator + demodulator*

Convierte señales digitales en analógicas y viceversa, como en líneas telefónicas tradicionales.

## ◆ Tipos de modulación

Tipo	Descripción	Ejemplo de uso
Analógica (AM, FM, PM)	Modifica amplitud, frecuencia o fase de una portadora.	Radio, TV, enlaces legacy.
Digital (ASK, FSK, PSK, QAM)	Representa bits alterando parámetros de la portadora.	Wi-Fi, ADSL, DOCSIS.

## ◆ Multiplexación

Permite compartir un mismo medio físico entre múltiples señales.

Método	Descripción
FDM (Frequency-Division Multiplexing)	Varias señales simultáneas en diferentes rangos de frecuencia.
TDM (Time-Division Multiplexing)	Cada señal usa el canal durante una fracción de tiempo alternada.

 En la recepción, el demodulador separa y reconstruye la señal original para convertirla nuevamente en datos digitales.

## 1 6 Conclusión de las capas inferiores

Capa	Función principal	Protocolos / Dispositivos
3 – Network	Direccionamiento lógico y enrutamiento entre redes	IP, ICMP, OSPF, routers
2 – Data Link	Transferencia libre de errores en la red local	Ethernet, PPP, switches
1 – Physical	Transmisión real de bits por medios físicos	Cables, hubs, modulación

# 1 7 Summary — Resumen del Capítulo 2

El **modelo OSI (Open Systems Interconnection)** es una arquitectura conceptual de **siete capas** que describe cómo los datos se mueven desde una aplicación en un dispositivo hasta otra aplicación en un dispositivo remoto.

Cada capa tiene una función definida y se comunica solo con las capas adyacentes.

## ◆ Estructura general del modelo

Grupo	Capas	Responsabilidad principal
Upper Layers (7–5)	Application, Presentation, Session	Interacción con el usuario, formato de datos, establecimiento de sesiones.
Lower Layers (4–1)	Transport, Network, Data Link, Physical	Transmisión real de datos y direccionamiento físico/lógico.

## ◆ Funciones clave de cada capa

Capa	Nombre	Función principal	Protocolos o ejemplos
7	<b>Application</b>	Servicios de red al usuario final	HTTP, FTP, DNS, SMTP
6	<b>Presentation</b>	Traducción, compresión y cifrado	SSL/TLS, JPEG, ASCII
5	<b>Session</b>	Establecimiento y control de sesiones	NetBIOS, RPC
4	<b>Transport</b>	Entrega confiable extremo a extremo	TCP, UDP
3	<b>Network</b>	Direccionamiento lógico y enrutamiento	IP, ICMP, OSPF
2	<b>Data Link</b>	Enlace físico, detección de errores	Ethernet, PPP
1	<b>Physical</b>	Transmisión de bits por el medio físico	Cables, hubs, modulación

 El modelo OSI es una referencia, no un estándar de implementación; los protocolos reales como TCP/IP se basan en él.

## ◆ Importancia práctica

- Proporciona una **guía universal** para diseñar e interpretar redes.
- Permite **identificar fallos**: por ejemplo, si un ping falla, el problema suele estar entre las capas 1 y 3.
- Facilita la **interoperabilidad** entre equipos y protocolos de distintos fabricantes.
- Ayuda a **estandarizar el desarrollo** de software y hardware de red.

# 1 8 Exam Essentials — Puntos clave para el examen

## 1. Comprender la función de cada capa OSI.

Debes ser capaz de describir qué hace cada capa y cómo se relaciona con las demás.

## 2. Reconocer ejemplos de protocolos por capa.

- Capa 7 → HTTP, DNS
- Capa 4 → TCP, UDP
- Capa 3 → IP, ICMP

- Capa 2 → Ethernet, PPP
- Capa 1 → Cableado, hubs

### 3. Diferenciar direccionamiento lógico y físico.

- Lógico: IP (Capa 3).
- Físico: MAC (Capa 2).

### 4. Identificar qué dispositivos operan en cada capa.

- Capa 1 → hubs, cables
- Capa 2 → switches
- Capa 3 → routers
- Capa 4–7 → firewalls de capa 7, proxys, gateways

### 5. Entender TCP vs UDP.

- TCP = confiable, orientado a conexión.
- UDP = no confiable, sin conexión.

### 6. Recordar el mnemónico del orden de capas:

“Please Do Not Throw Sausage Pizza Away” (de la 1 a la 7).

## 1 | 9 Written Lab — Actividad escrita

### Ejercicio 1:

Enumera las siete capas del modelo OSI **de la capa más baja a la más alta** y explica la función principal de cada una.

### Ejercicio 2:

Para cada protocolo, indica la capa en la que opera:

- HTTP
- TCP
- IP
- Ethernet
- DNS
- UDP
- ICMP

### Ejercicio 3:

Describe la diferencia entre **direcciónamiento lógico (IP)** y **direcciónamiento físico (MAC)**, indicando en qué capa se utilizan.

### Ejercicio 4:

Explica brevemente cómo una aplicación de correo electrónico (SMTP/POP3) utiliza el modelo OSI desde la capa 7 hasta la capa 1 para enviar un mensaje.

 Consejo para el examen: al diagnosticar un problema de red, identifica **en qué capa deja de funcionar** la comunicación. Esto facilita aislar la causa.

## 2 | 0 Written Lab — Solución desarrollada

## Ejercicio 1 — Capas del modelo OSI (de la más baja a la más alta)

Nº	Capa	Función principal
1	<b>Physical</b>	Define medios físicos, señales eléctricas/ópticas, conectores y velocidad de transmisión. Transmite bits crudos.
2	<b>Data Link</b>	Proporciona transferencia libre de errores entre nodos. Usa direcciones MAC y controla el acceso al medio.
3	<b>Network</b>	Gestiona el direccionamiento lógico (IP) y determina rutas entre redes (enrutamiento).
4	<b>Transport</b>	Segmenta datos, asegura entrega confiable, gestiona control de flujo y corrección de errores.
5	<b>Session</b>	Crea, mantiene y finaliza sesiones entre aplicaciones. Controla el diálogo (simplex, half/full-duplex).
6	<b>Presentation</b>	Traduce, cifra y comprime los datos. Garantiza que el formato sea entendible para ambos sistemas.
7	<b>Application</b>	Ofrece servicios de red a las aplicaciones del usuario (HTTP, FTP, DNS, etc.).

 Mnemónico: Please Do Not Throw Sausage Pizza Away

(Physical → Data Link → Network → Transport → Session → Presentation → Application)

## Ejercicio 2 — Protocolos y su capa correspondiente

Protocolo	Capa OSI	Descripción breve
HTTP	7 – Application	Protocolo para la comunicación web cliente-servidor.
TCP	4 – Transport	Protocolo orientado a conexión y fiable.
IP	3 – Network	Define direcciones lógicas y enrutamiento de paquetes.
Ethernet	2 – Data Link	Protocolo LAN basado en tramas con dirección MAC.
DNS	7 – Application	Traduce nombres de dominio en direcciones IP.
UDP	4 – Transport	Protocolo sin conexión, rápido, sin control de errores.
ICMP	3 – Network	Protocolo de control y diagnóstico (ping, traceroute).

 Si puedes asociar cada protocolo con su capa, será más sencillo identificar dónde puede fallar una comunicación.

## Ejercicio 3 — Direccionamiento lógico vs físico

Tipo de direccionamiento	Capa	Descripción	Ejemplo
Lógico (IP)	3 – Network	Permite identificar dispositivos en distintas redes y enrutar paquetes a través de múltiples saltos.	192.168.1.25 , 2001:db8::1
Físico (MAC)	2 – Data Link	Identifica de forma única cada dispositivo dentro de una red local (LAN). No cambia, viene grabada en la NIC.	00:1A:2B:3C:4D:5E

 *El direccionamiento IP cambia con la red; el MAC es permanente y actúa dentro del enlace local.*

## Ejercicio 4 — Flujo del modelo OSI en una aplicación de correo electrónico (SMTP/POP3)

### Escenario:

Un usuario envía un correo mediante **SMTP** y el receptor lo descarga con **POP3**.

Capa	Acción / Función en el proceso de envío
7 – Application	El cliente de correo usa <b>SMTP</b> para enviar el mensaje y el servidor lo recibe mediante <b>POP3 o IMAP</b> .
6 – Presentation	El mensaje se convierte a un formato estándar (texto plano o MIME) y se cifra con <b>TLS</b> si está habilitado.
5 – Session	Se abre una sesión entre el cliente y el servidor SMTP. Se sincroniza el flujo de mensajes.
4 – Transport	<b>TCP</b> divide el mensaje en segmentos y controla que lleguen íntegros (ACK, control de flujo).
3 – Network	<b>IP</b> define la dirección origen/destino y selecciona la mejor ruta al servidor remoto.
2 – Data Link	<b>Ethernet o Wi-Fi</b> encapsula los paquetes IP en tramas con direcciones MAC.
1 – Physical	Los bits viajan físicamente por el cable o medio inalámbrico hasta el router o el servidor remoto.

 *Al recibir el correo, el proceso ocurre a la inversa: los datos se desempaquetan desde la capa 1 hasta la capa 7.*

## 2 | 1 Review Questions — Chapter 2

1

Which layer of the OSI model is responsible for reliable end-to-end delivery of data?

¿Qué capa del modelo OSI es responsable de la entrega confiable de datos de extremo a extremo?

Opciones:

- A. Session
- B. Transport
- C. Network
- D. Data Link

 **Respuesta correcta:** B. Transport

Explicación:

La **capa 4 (Transport)** segmenta los datos, controla errores y flujo, y confirma la entrega mediante TCP.

2

At which OSI layer do routers primarily operate?

¿En qué capa OSI operan principalmente los routers?

- A. Data Link
- B. Network
- C. Transport
- D. Physical

B. Network

**Explicación:**

Los routers usan **direcciónamiento IP y protocolos de enrutamiento** (OSPF, BGP) que pertenecen a la **capa 3**.

---

3

**Which OSI layer defines the protocols used for email (SMTP, POP3, IMAP)?**

**¿Qué capa define los protocolos usados para correo electrónico (SMTP, POP3, IMAP)?**

- A. Application
- B. Presentation
- C. Session
- D. Transport

A. Application

**Explicación:**

Los servicios de aplicación se implementan en la **capa 7**, la interfaz directa entre usuario y red.

---

4

**Which OSI layer converts data into signals for transmission across the medium?**

**¿Qué capa convierte los datos en señales para su transmisión a través del medio físico?**

- A. Data Link
- B. Physical
- C. Network
- D. Transport

B. Physical

**Explicación:**

La **capa 1** define las características eléctricas, ópticas o de radio necesarias para enviar bits.

---

5

**What address type is used at the Data Link layer?**

**¿Qué tipo de dirección se usa en la capa Data Link?**

- A. Logical (IP)
- B. Physical (MAC)
- C. Port number
- D. Hostname

B. Physical (MAC)

## **Explicación:**

Las tramas de capa 2 emplean **direcciones MAC** de 48 bits para identificar dispositivos locales.

---

**6**

**Which OSI layer is responsible for establishing, managing, and terminating sessions?**

**¿Qué capa se encarga de establecer, administrar y finalizar sesiones?**

- A. Transport
- B. Network
- C. Session
- D. Application

**✓ C. Session**

## **Explicación:**

La **capa 5** controla los diálogos entre aplicaciones y mantiene separadas las sesiones múltiples.

---

**7**

**At which layer does data segmentation occur?**

**¿En qué capa ocurre la segmentación de datos?**

- A. Application
- B. Transport
- C. Network
- D. Data Link

**✓ B. Transport**

## **Explicación:**

El protocolo TCP divide la información en **segmentos**, numerándolos para permitir su reensamblado.

---

**8**

**Which of the following operates at Layer 2 of the OSI model?**

**¿Cuál de los siguientes opera en la capa 2 del modelo OSI?**

- A. Router
- B. Switch
- C. Hub
- D. Repeater

**✓ B. Switch**

## **Explicación:**

Los **switches** usan direcciones MAC y reenvían tramas dentro de una red LAN (capa Data Link).

---

**9**

**Which layer handles encryption and decryption of data for secure transmission?**

**¿Qué capa maneja el cifrado y descifrado de los datos para una transmisión segura?**

- A. Session
- B. Presentation
- C. Application
- D. Transport

**B. Presentation**

**Explicación:**

La **capa 6** se encarga de la **traducción, compresión y cifrado** (ej. TLS/SSL).

10

**What is the PDU (Protocol Data Unit) name used at the Network layer?**

**¿Cómo se denomina la unidad de datos en la capa Network?**

- A. Frame
- B. Packet
- C. Segment
- D. Bit

**B. Packet**

**Explicación:**

La **capa 3** encapsula segmentos en **paquetes** que incluyen direcciones IP de origen y destino.

1 1

**Which layer uses port numbers to identify applications?**

**¿Qué capa usa números de puerto para identificar aplicaciones?**

- A. Application
- B. Transport
- C. Session
- D. Network

**B. Transport**

**Explicación:**

Los puertos (80, 443, 25...) pertenecen a la **capa 4**, donde TCP/UDP diferencian procesos de aplicación.

1 2

**Which OSI layer ensures that data is delivered in the correct order?**

**¿Qué capa garantiza que los datos se entreguen en el orden correcto?**

- A. Network
- B. Session
- C. Transport
- D. Data Link

**C. Transport**

**Explicación:**

TCP utiliza números de secuencia para **reordenar segmentos** y asegurar la entrega coherente.

1 3

What type of communication allows data flow in both directions simultaneously?

¿Qué tipo de comunicación permite el flujo de datos en ambos sentidos de forma simultánea?

- A. Simplex
- B. Half-duplex
- C. Full-duplex
- D. Serial

C. Full-duplex

**Explicación:**

Definido por la **capa 5 (Session)**, permite transmisión y recepción al mismo tiempo.

1 4

Which device regenerates and amplifies signals without examining the data?

¿Qué dispositivo regenera y amplifica señales sin examinar los datos?

- A. Bridge
- B. Router
- C. Repeater
- D. Switch

C. Repeater

**Explicación:**

Un **repetidor** trabaja en la **capa 1**, extendiendo la señal física sin interpretar tramas ni direcciones.

1 5

At which OSI layer does IP addressing occur?

¿En qué capa ocurre el direccionamiento IP?

- A. Data Link
- B. Network
- C. Transport
- D. Session

B. Network

**Explicación:**

El **IP (Internet Protocol)** define direcciones lógicas y pertenece a la **capa 3**.

1 6

Which OSI layer is responsible for framing?

¿Qué capa es responsable del “framing” (encapsulación en tramas)?

- A. Network
- B. Data Link
- C. Physical
- D. Transport

## B. Data Link

**Explicación:**

La **capa 2** encapsula paquetes en **frames**, añade encabezados/tráilers y controla errores.

---

1 7

**What OSI layer defines cabling standards and connectors (e.g., RJ-45)?**

**¿Qué capa define los estándares de cableado y conectores (p. ej., RJ-45)?**

- A. Data Link
- B. Network
- C. Physical
- D. Transport

## C. Physical

**Explicación:**

La **capa 1** especifica conectores, voltajes, pines y longitudes de cable.

---

1 8

**Which protocol is connectionless and offers no reliability?**

**¿Qué protocolo es sin conexión y no ofrece fiabilidad?**

- A. TCP
- B. UDP
- C. ICMP
- D. IPsec

## B. UDP

**Explicación:**

UDP no realiza handshake ni comprobaciones de entrega; prioriza la **velocidad** (streaming, VoIP).

---

1 9

**Which OSI layer provides the means for data compression?**

**¿Qué capa proporciona los medios para la compresión de datos?**

- A. Application
- B. Presentation
- C. Session
- D. Transport

## B. Presentation

**Explicación:**

La **capa 6** puede comprimir archivos o flujos para optimizar el ancho de banda.

---

2 0

**At which OSI layer does the Ping utility operate?**

**¿En qué capa OSI opera la utilidad Ping?**

- A. Network
- B. Transport
- C. Data Link
- D. Session

 A. Network

**Explicación:**

Ping usa ICMP, protocolo de diagnóstico de la **capa 3**, para comprobar la conectividad IP.

---

 Fin del Capítulo 2 — The Open Systems Interconnection Model